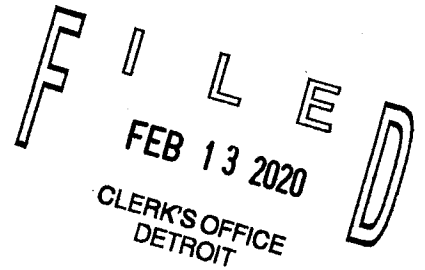


26

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION



UNITED STATES OF AMERICA

v.

Cr. No. 19-20478

D-1 ALEKSANDR GRICHISHKIN,

Hon. Denise Page Hood

D-2 ANDREI SKVORTSOV,

OFFENSES:

D-3 ALEKSANDR SKORODUMOV,

RICO Conspiracy; 18 U.S.C.
§1962(d)

D-4 PAVEL STASSI,

Bank Fraud Conspiracy; 18
U.S.C. §1349

Defendants.

RICO Forfeiture; 18 U.S.C.
§1963

FIRST SUPERSEDING INDICTMENT

THE GRAND JURY CHARGES THAT:

GENERAL ALLEGATIONS

At all times relevant to this First Superseding Indictment:

1. Defendant ALEKSANDR GRICHISHKIN was a Russian national.
2. Defendant ANDREI SKVORTSOV was a Russian national.
3. Defendant ALEKSANDR SKORODUMOV was a Lithuanian national.

4. Defendant PAVEL STASSI was an Estonian national.

OVERVIEW OF THE DEFENDANTS' CRIMINAL SCHEME

5. As set forth more fully below, Defendants GRICHISHKIN, SKVORTSOV, SKORODUMOV, and STASSI were members of a CRIMINAL ORGANIZATION (hereafter, "ORGANIZATION"). The ORGANIZATION was a so-called "bulletproof hosting" service using computers in the United States, and elsewhere.

6. As a bulletproof hosting service, the ORGANIZATION rented to cyber-criminal clients Internet Protocol ("IP") addresses and servers, and registered domain names (hereafter, "Internet infrastructure"), in a manner designed to preserve both the ORGANIZATION and its clients' anonymity, to minimize interruptions in service, and to help the clients evade detection of their criminal activities by law enforcement. That is, the ORGANIZATION and its members rented Internet infrastructure to clients knowing this infrastructure would be used to commit cybercrimes.

7. Further, as a bulletproof hosting service, the ORGANIZATION's members provided various services to the ORGANIZATION's criminal clientele. One such service included monitoring "abuse notices" and "block lists" issued or maintained by third-party online services, including Spamhaus and Zeus Tracker, which reported malicious activities on particular domains and IP addresses and

caused Internet Service Providers (“ISPs”) not to route traffic to the affected domains or IP addresses until the “block” was removed or the abuse notice resolved. The ORGANIZATION’s members monitored these lists and notices so they could quickly identify “flagged” or blocked domains and IP addresses, and transfer their clients’ affected infrastructure to new or “clean” domains and IP addresses to minimize interruptions in service.

8. As members of the ORGANIZATION and as set forth in greater detail below, Defendants GRICHISHKIN, SKVORTSOV, SKORODUMOV, and STASSI knowingly facilitated and aided and abetted the distribution over the Internet of “spam” email and malicious software (“malware”), including “banking trojans,” and the hosting of “exploit kits,” that were used to gain unauthorized access to victims’ computers in the United States and abroad and commit financial frauds.

9. Defendants GRICHISHKIN, SKVORTSOV, SKORODUMOV, and STASSI knew that the ORGANIZATION’s Internet infrastructure and services were used by their clients to further computer intrusion activity and resulting financial frauds, including fraud of financial institutions and their account holders, in the United States, and acted with the purpose of aiding such crimes, and with the intention of causing such crimes to occur.

10. Comerica Bank, NBT Bank, Silicon Valley Bank, PNC Bank, JP Morgan Chase, and Bank of America, among others, were federally insured United States financial institutions as defined by 18 U.S.C. Section 20.

OVERVIEW OF RELEVANT CYBERCRIMES AND TERMS

Banking Trojans

11. Banking trojans are a form of malware typically designed to gain unauthorized access to victims' computers and steal personal information, including account holders' usernames, passwords, and other personally identifiable information used to access and control online bank accounts. Banking trojans are often disseminated through spam email messages from seemingly benign senders containing what appears to be harmless attachments or hyperlinks to harmless webpages. When a victim opens such an attachment or clicks on a hyperlink and visits the linked webpage, additional malware is downloaded and installed on the victim's computer without the victim's knowledge or consent, which provides further instructions to the victim's computer.

12. Once installed, this additional malware steals user names, passwords, and other information stored on the computer or entered into webpages by the victim account holder. The malware then causes this information to be sent to a computer controlled by the cyber criminals, who use the information to log into the victim's bank accounts without authorization and steal, and attempt to steal, money

from these bank accounts. Banking trojans can be tailored by cyber criminals to steal online banking credentials for accounts with specific financial institutions.

13. The ORGANIZATION aided others in proliferating banking trojans, which included “Zeus” “SpyEye,” “Dyre,” and “Citadel,” among others.

Collectively, these trojans infected computers around the world, including in the United States; targeted numerous financial institutions in the United States, including at least one U.S. financial institution located in the Eastern District of Michigan; and caused millions of dollars in losses.

Exploit Kits

14. Exploit kits are used to identify vulnerabilities in victims’ computers, exploit such vulnerabilities to gain unauthorized access to the computers, and then deliver additional malware to the computers. As with other forms of malware, a victim’s computer typically is infected when the victim unwittingly opens an attachment, clicks on a hyperlink, or visits a compromised webpage, which redirects the victim to a computer server on which the exploit kit is hosted. The exploit kit scans the victim’s computer for vulnerabilities, which are then used to further access and deliver additional malware to the victim’s computer.

15. The ORGANIZATION aided others in proliferating the Blackhole Exploit Kit, which was used by cyber criminals to access without authorization

computers in the United States and abroad, and to disseminate malware designed to steal victims' banking credentials, including the Zeus trojan.

Botnets

16. Cyber criminals disseminating malware often create "botnets" (or networks of compromised computers, or "bots") by infecting victims' computers with malware that allows the cyber criminals to control each bot without the victim's knowledge or authorization.

17. The ORGANIZATION knowingly provided its clients with the Internet infrastructure necessary to form botnets, which the ORGANIZATION knew would be used to steal information from infected computers and transmit spam emails, among other things.

Spam

18. Spam is unsolicited bulk email that is transmitted over the Internet in a manner that hides the true source of the spam and the identity of the individuals who send it ("spammers"). Spam is often a means by which cyber criminals distribute malware over the Internet.

19. The ORGANIZATION's bulletproof hosting service was used by cyber criminals to transmit spam over the Internet, which the ORGANIZATION's members knew was being used to disseminate malware to unsuspecting victims in the United States and abroad.

THE CRIMINAL ORGANIZATION

20. At various times relevant to this First Superseding Indictment, Defendants GRICHISHKIN, SKVORTSOV, SKORODUMOV, and STASSI, and others known and unknown to the Grand Jury, were members of the ORGANIZATION, whose members aided and abetted bank fraud, wire fraud affecting financial institutions, computer fraud, and trafficking in unauthorized access devices, and whose members used and trafficked in counterfeit and stolen identification documents. Members of the ORGANIZATION operated throughout the world, including in the Eastern District of Michigan.

21. Defendants SKVORTSOV and GRICHISHKIN launched the ORGANIZATION by at least August 2008. The ORGANIZATION provided bulletproof hosting services to cyber criminals through at least November 2015.

ROLE OF THE DEFENDANTS AND CO-CONSPIRATORS

22. The ORGANIZATION's members had defined roles in the ORGANIZATION. Defendants GRICHISHKIN, SKVORTSOV, SKORODUMOV, and STASSI, and other persons known and unknown to the Grand Jury, participated in the operation and management of the ORGANIZATION as follows:

Proprietors

23. Defendants SKVORTSOV and GRICHISHKIN launched the

ORGANIZATION in or about 2008, and were its proprietors.

24. GRICHISHKIN was the ORGANIZATION's day-to-day leader. He oversaw advertising on online cybercrime forums, set pricing for hosting services, negotiated and interfaced with clients, managed employee hiring and compensation, and supervised the systems administrators' and other employees' work.

25. SKVORTSOV served as a reference for the ORGANIZATION on online cybercrime forums, where businesses' success depended upon reputations and relationships; referred criminal clients; proposed business ideas; and served as a point-of-contact for important clients, or when there were problems with the ORGANIZATION's bulletproof hosting services.

Systems Administrators

26. The ORGANIZATION employed multiple systems administrators who registered domains, set up and configured servers, assigned IP addresses, provided technical assistance to clients, and reconfigured clients' Internet infrastructure in response to abuse notices. Systems administrators sometimes provided false information to ISPs from which the ORGANIZATION rented Internet infrastructure to avoid interruptions in service, and assisted other ORGANIZATION members in doing the same.

27. SKORODUMOV was systems administrator for the

ORGANIZATION from at least December 2009 until at least May 2012.

Client Relations and Administrative Personnel

28. The ORGANIZATION employed client relations and administrative personnel who conducted and tracked advertising efforts, screened job applications for new hires, used stolen personally identifiable information and false information to register financial accounts and webhosting accounts with ISPs, and communicated with ISPs about abuse notices relating to the ORGANIZATION's customers' accounts.

29. STASSI performed client relations and administrative services from on or about November 2010 through at least September 2014. Under GRICHISHKIN's supervision, STASSI screened job applicants, advertised on cybercrime forums, leased webhosting services from ISPs using fraudulent information, received client orders for bulletproof hosting services, registered domains, and provided some technical support to clients.

COUNT 1

18 U.S.C. § 1962(d)

Conspiracy to Engage in a Racketeer Influenced Corrupt Organization

D-1 ALEKSANDR GRICHISHKIN

D-2 ANDREI SKVORTSOV

D-3 ALEKSANDR SKORODUMOV

D-4 PAVEL STASSI

30. Paragraphs 1 through 29 are incorporated by reference as fully set

forth herein.

31. The ORGANIZATION, including its leadership, membership, and associates, constituted an “enterprise,” as defined by Title 18, United States Code, Section 1961(4), that is, a group of individuals associated in fact, although not a legal entity. The enterprise constituted an ongoing organization whose members functioned as a continuing unit for a common purpose of achieving the objectives of the enterprise. The enterprise was engaged in, and its activities affected, interstate and foreign commerce.

PURPOSES OF THE ENTERPRISE

32. The purposes of the enterprise included, but were not limited to, the following:

A. Providing Internet infrastructure and services for cyber criminals whom the ORGANIZATION’s members knew to be using these services for illegal activities, including bank fraud, wire fraud, computer fraud, and trafficking in unauthorized access devices;

B. Promoting the ORGANIZATION, its services, and the reputation and standing of its members;

C. Protecting the enterprise, its members, and its clients from detection, apprehension, and prosecution by law enforcement; and

D. Enriching the leaders and members of the enterprise by taking a fee for services rendered for the ORGANIZATION's clients, which the enterprise members knew furthered the criminal activities of those clients.

MEANS AND METHODS OF THE ENTERPRISE

33. The means and methods by which Defendants GRICHISHKIN, SKVORTSOV, SKORODUMOV, and STASSI, and other members of the enterprise conducted and participated in the conduct of the affairs of the enterprise included, but were not limited to, the following:

A. The ORGANIZATION's members advertised bulletproof hosting services to known cyber criminals and on known online cybercrime forums, including but not limited to LCP, Mazafaka, Direct Connection, Verified, and Vor, between at least 2008 and at least 2013. The ORGANIZATION addressed some of these advertisements to "Gentlemen-Fraudsters." The forums on which the advertisements were posted could be accessed by forum members from computers located anywhere in the world, including in the Eastern District of Michigan, and were used by those members to buy, sell, or rent malware kits, botnets, and stolen personally identifiable information, and related services. For example:

i. On or about July 30, 2009, SKVORTSOV and GRICHISHKIN posted or caused to be posted an advertisement on the Russian-language cybercrime forum, LCP, which stated, in part:

We can support all types of projects (all listings like Spamhaus or ZeusTracker are ignored):

- any malware (trojans, virii, sockbots, spambots etc)
- any traffic needs (tds, sploits, iframers etc)
- any input & output spam (direct spam from servers, socks spam, spamvertised projects[.])

ii. On or about December 29, 2010, GRICHISHKIN and

STASSI discussed an advertisement for the ORGANIZATION that stated

(in part):

We are glad to present our hosting services (and associated services) to you for your problem projects.

...

Thus, we finish our prelude and begin in earnest regarding: "who we are."

1) A full spectrum of hosting services – dedicated servers, domains, hosting (shared and vps), ssl certificates (thawte, geotrust). All services are resistant to various kinds of provocation from your foes and other slackers.

2) Everyone's favorite locations: Latvia, Germany, China, Singapore, Malaysia, Hong Kong, Iran, Holland, Luxembourg, USA. . . .

3) There is the capability to set up practically any hardware. . . .

4) On many platforms we have our own automated systems and IP addressing. We really handle abuses and process them without damage to clients.

5) We have direct, clean, legal relationships with providers and data centers. Moreover, everyone is always kept apprised of what they are doing and why.

6) We do not mix black and white. That means, for example, if there is a FireEye holy war on malware guys, the work of other clients will not be blocked. We have built the utmost distributed structure and it has been tested on real operations.

7) We are true specialists in our business; that is why we will not lag behind in any kind of advanced task (be it a special API for your software, a highload solution, non-standard hardware firewalls, or even simply kvm – it is all within our capabilities).

8) We essentially have twenty-four hour support on ICQ and Jabber; only one contact that is always up to date on your situation, responds to and resolves our common issues, and always sees and receives your messages.

9) Our systems administrators provide free assistance to clients (within reason).

...

Regarding project topics – everything is possible except Child Porn.

The most popular content-solutions:

- Spam (xrunder, dorgens),
- Spam objects (doorways, splogs),
- Running traffic (TDS),
- Licensing problems (pharma),
- Copyright problems (warez, MP3),
- Malware (codex, anti-spy),
- Adult (rape, zoo)

And much more . . .

STASSI maintained copies of the ORGANIZATION's advertisements, as well as a robust spreadsheet that he used to track all of the ORGANIZATION's advertisements.

iii. On or about April 4, 2010, at SKVORTSOV's direction, GRICHISHKIN contacted the developer of the SpyEye banking trojan, "offer[ing] to collaborate" and proposing "you can refer clients to us and I will payout a fixed amount for each one."

B. ORGANIZATION members leased domains, servers, and IP

addresses from ISPs all over the world, including in the United States, using stolen and fraudulent identity information and a variety of payment methods, so as to hide the true owners and users of the accounts. For example:

i. From at least September 2011 until at least January 2018, ORGANIZATION members used a PayPal account to rent Internet infrastructure from hundreds of ISPs. This PayPal account was registered to the stolen or fraudulent identity of "I.P.," using a Google email address in I.P.'s name and scans of two fraudulent Lithuanian passports in I.P.'s name. In 2015, an IP address leased by the ORGANIZATION using the fraudulent "I.P." identity and PayPal account was used to steal funds from, or attempt to steal funds from, U.S. bank accounts at Silicon Valley Bank, JP Morgan Chase, PNC Bank, and Bank of America. The account holders' computers were infected with Dyre, a banking trojan.

ii. On or about September 15, 2011, STASSI directed another ORGANIZATION member to register various domain names, using different information for each registration. Three months later, on or about December 29, 2011, ORGANIZATION members received an abuse notice from a U.S. service provider indicating that it was no longer routing traffic to a server rented by the ORGANIZATION because one of these domains STASSI had ordered be registered was hosting "ZeuS webinjects."

iii. In or about November 2011, STASSI knowingly used a fraudulent utility bill and the stolen United States passport of “C.D.,” a real person, to register a web-hosting account with OVH, a French ISP, which remained active until January 6, 2014.

C. ORGANIZATION members subleased the Internet infrastructure it had rented from ISPs to individuals whom they knew were using this infrastructure to disseminate spam and malware, including banking trojans and exploit kits; to operate botnets; and to steal banking credentials. For example:

i. Between in or about July 2009 and at least March 2010, ORGANIZATION members rented domains, servers, and IP addresses to members of the so-called “Jabberzeus Crew,” who used this infrastructure to disseminate Zeus malware, steal online banking credentials, and steal, or attempt to steal, funds from U.S. victims’ accounts, including accounts with Comerica Bank, a financial institution located in the Eastern District of Michigan. GRICHISHKIN agreed to lease infrastructure to the Jabberzeus Crew knowing that it would be used “for botnets [that] get downloaded from spam,” “for Zeus,” and for “bots” that “spam U.S. government entities.”

D. ORGANIZATION members assisted clients to configure their Internet infrastructure so as to avoid detection and interruptions in service, and maximize profits.

i. For example, in or about August 2011 and April 2012, respectively, SKORODUMOV helped clients set up SpyEye and Citadel malware-related infrastructure, knowing this infrastructure would be used to set up botnets and steal victims' banking credentials.

E. ORGANIZATION members monitored third-party online services' "block lists," including Spamhaus and Zeus Tracker, which periodically flagged domains and IP addresses administered by the ORGANIZATION as being used for malicious activities, and caused ISPs not to route traffic to or from the affected domains or IP addresses until the "block" was removed or the abuse notice resolved. ORGANIZATION members also notified affected clients when the ORGANIZATION's members became aware that an ORGANIZATION-administered domain or IP address was included on a block list or was the subject of an abuse notice, relocating the clients' data to new Internet infrastructure, and providing false information to the ISPs from which the ORGANIZATION had rented the Internet infrastructure so as to avoid an interruption in or discontinuation of service. For example:

i. On or about March 21, 2010, GRICHISHKIN forwarded an abuse notice, which flagged one of the ORGANIZATION's domains as hosting Zeus botnet files, to another ORGANIZATION member.

GRICHISHKIN instructed the ORGANIZATION member to "[m]ove it to

an adjacent IP.”

ii. On or about January 15, 2012, GRICHISHKIN instructed SKORODUMOV on how to respond to abuse notices and advise clients regarding service interruptions:

Regarding SPY/Zeus/Blackhole, we change IPs . . . / Regarding other abuses – it’s better to say that it’s something else, but not a complaint. Like, the domain was locked by the registrar; the domain is being filtered, and so on. . . . [F]or SPY/Zeus/Blackhole, you can say it this way: your IP was taken down due to [Spamhaus Block List] and there will be a replacement. / . . . / For everyone that has Blackhole, the replacement is strictly to be paid for. / Zeus and SPY can be changed immediately for free.

F. ORGANIZATION members used online payment accounts often registered with false information to receive payments from clients and pay staff members’ salaries in order to protect the membership’s anonymity.

G. ORGANIZATION members used a wide range of communication methods, and changed accounts frequently, in order to protect the membership’s anonymity and to avoid detection by law enforcement. Many of these communications accounts were registered using false information or online aliases. The communications methods used by ORGANIZATION members included but were not limited to:

- i. Postings on private, invitation-only online cybercrime forums under a variety of online aliases;
- ii. Private messaging, including Jabber and ICQ, which are often encrypted and, in the case of Jabber, frequently hosted on private servers so as to decrease the risk that backups and logs can be obtained through legal process or seized by law enforcement; and
- iii. Email and other communications accounts with commercial providers, often registered using false or stolen information.

THE RACKETEERING CONSPIRACY

34. Beginning no later than in or around August 2008 and continuing to at least November 2015, in the Eastern District of Michigan and elsewhere, Defendants ALEKSANDR GRICHISHKIN, ANDREI SKVORTSOV, ALEKSANDR SKORODUMOV, PAVEL STASSI, and other persons, known and unknown to the Grand Jury, being persons employed by and associated with the ORGANIZATION, an enterprise, which engaged in, and the activities of which affected, interstate and foreign commerce, knowingly and intentionally conspired to violate Title 18, United States Code, Section 1962(c), that is, to conduct and participate, directly and indirectly, in the conduct of the affairs of that enterprise through a pattern of racketeering activity, as that term is defined in Title 18, United States Code, Sections 1961(1) and (5), consisting of multiple acts indictable under

18 U.S.C. § 1028 (fraud in connection with identification documents), 18 U.S.C. § 1029 (fraud in connection with access devices), 18 U.S.C. § 1030(a)(5)(A) (computer fraud), 18 U.S.C. § 1343 (wire fraud affecting a financial institution), and 18 U.S.C. § 1344 (bank fraud).

35. It was a part of the conspiracy that each Defendant agreed that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the enterprise.

All in violation of Title 18, United States Code, Section 1962(d).

COUNT 2
18 U.S.C. § 1349
Bank Fraud Conspiracy

D-1 ALEKSANDR GRICHISHKIN
D-2 ANDREI SKVORTSOV
D-3 ALEKSANDR SKORODUMOV
D-4 PAVEL STASSI

36. Paragraphs 1 through 29 are incorporated by reference as fully set forth herein.

37. From in or about August 2008 until at least November 2015, the exact dates being unknown to the Grand Jury, ALEKSANDR GRICHISHKIN, ANDREI SKVORTSOV, ALEKSANDR SKORODUMOV, PAVEL STASSI, and other co-conspirators not named as defendants herein, knowingly agreed to execute, and attempt to execute, a scheme to defraud a wide range of U.S. financial institutions,

and their account holders, including Comerica Bank in the Eastern District of Michigan, and to obtain the money, funds and other property owned by and under the control of those U.S. financial institutions by means of material false or fraudulent pretenses, representations, and promises.

38. It was part of the scheme that the co-conspirators used computer intrusions, malicious software, and fraud to steal, or attempt to steal, millions of dollars from several bank accounts in the United States, and elsewhere. The co-conspirators infected computers with software that captured passwords, account numbers, and other information necessary to log into online banking accounts, and then used the captured information to steal, and to attempt to steal, funds from accounts held with U.S. financial institutions, including Comerica Bank in the Eastern District of Michigan.

39. It was part of the scheme that GRICHISHKIN, SKVORTSOV, SKORODUMOV, and STASSI registered domain names for and leased IP addresses and servers to these co-conspirators, and directed other ORGANIZATION members to do so, and configured and administered this Internet infrastructure for the co-conspirators. GRICHISHKIN, SKVORTSOV, SKORODUMOV, and STASSI knew and intended that this Internet infrastructure would be used by the co-conspirators to disseminate malicious software, conduct

computer intrusions, and steal, and attempt to steal, funds from bank accounts in the United States, and elsewhere.

40. Between August 2008 until at least November 2015, GRICHISHKIN, SKVORTSOV, SKORODUMOV, and STASSI knowingly agreed to execute, and attempt to execute, the scheme set forth above, in that Defendants GRICHISHKIN, SKVORTSOV, SKORODUMOV, and STASSI agreed to, and did, host and service Internet infrastructure that was used by the co-conspirators to disseminate banking trojans, including Zeus, SpyEye, Dyre, and Citadel; receive stolen banking credentials that had been transferred without authorization from computers infected with these malware; and access U.S. financial institution accounts without authorization; and these co-conspirators falsely represented to U.S. financial institutions that the co-conspirators were entitled to authorize transfers of funds out of bank accounts maintained with these financial institutions.

All in violation of Title 18, United States Code, Section 1349.

FORFEITURE ALLEGATIONS

18 U.S.C. § 1963, 18 U.S.C. § 982, and
18 U.S.C. § 981 together with 28 U.S.C. § 2461

41. The allegations contained in Counts One and Two of this First Superseding Indictment are hereby repeated, re-alleged, and incorporated by

reference herein as though fully set forth at length for the purpose of alleging forfeiture pursuant to the provisions of Title 18, United States Code, Sections 1963, 982(a)(2)(A), and 981(a)(1)(C) together with Title 28, United States Code, Section 2461.

42. Pursuant to Rule 32.2, Fed. R. Crim. P., notice is hereby given to the defendants that the United States will seek forfeiture as part of any sentence in accordance with Title 18, United States Code, Sections 1963, 982(a)(2)(A), and 981(a)(1)(C) together with Title 28, United States Code, Section 2461, in the event of any defendant's conviction under Counts One and Two of this First Superseding Indictment.

43. Upon conviction of Count One of this First Superseding Indictment, the Defendants, ALEKSANDR GRICHISHKIN, ANDREI SKVORTSOV, ALEKSANDR SKORODUMOV, and PAVEL STASSI, shall forfeit the following to the United States, pursuant to Title 18, United States Code, Sections 1963(a)(1)-(3):

A. any interest acquired or maintained in violation of section 1962, which interests are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 1963(a)(1);

B. any interest in, security of, claim against, or property or contractual right of any kind affording a source of influence over, any enterprise which the

defendant[s] established, operated, controlled, conducted, or participated in the conduct of, in violation of section 1962, which interests are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 1963(a)(2); and

C. any property constituting, or derived from, any proceeds obtained, directly or indirectly, from racketeering activity in violation of 1962, which interests are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 1963(a)(3);

44. Upon conviction of the offense in violation of Title 18, United States Code, Section 1349 set forth in Count Two of this First Superseding Indictment, the Defendants, ALEKSANDR GRICHISHKIN, ANDREI SKVORTSOV, and ALEKSANDR SKORODUMOV, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(A) or Title 18, United States Code, Section 981(a)(1)(C) together with Title 28, United States Code, Section 2461(c), any property constituting, or derived from, proceeds obtained, directly or indirectly, as a result of such violation.

45. If any of the above-described forfeitable property, as a result of any act or omission of the Defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;

- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 1963(m) and Title 21, United States Code, Section 853(p) as incorporated by Title 28, United States Code, Section 2461, to seek forfeiture of any other property of said Defendants up to the value of the above forfeitable property.

46. Money Judgment. Upon conviction of one or more violations alleged in this First Superseding Indictment, the United States will seek a forfeiture money judgment against the convicted Defendants in an amount representing the total amount of proceeds obtained as a result of Defendants' offenses.

All pursuant to Title 18, United States Code, Sections 1963, 982(a)(2)(A), and Title 18, United States Code, Section 981(a)(1)(C) together with Title 28, United States Code, Section 2461, and Rule 32.2, Federal Rules of Criminal Procedure.

THIS IS A TRUE BILL.

s/Grand Jury Foreperson
GRAND JURY FOREPERSON

MATTHEW SCHNEIDER
United States Attorney
Eastern District of Michigan

BRIAN BENCZKOWSKI
Assistant Attorney General,
Criminal Division

s/John K. Neal
JOHN K. NEAL
Chief, White Collar Crime Unit

s/John Lynch
JOHN LYNCH
Chief, Computer Crime and
Intellectual Property Section

s/Patrick E. Corbett
PATRICK E. CORBETT
Assistant United States Attorney

s/Louisa Marion
LOUISA MARION
Senior Counsel, Computer Crime and
Intellectual Property Section

Dated: 2/13/2020

United States District Court
Eastern District of Michigan**Criminal Case Cover Sheet****Case Number**
19-20478

NOTE: It is the responsibility of the Assistant U.S. Attorney signing this form to complete it accurately in all respects.

Companion Case Information	Companion Case Number:
This may be a companion case based upon LCrR 57.10 (b)(4) ¹ :	Judge Assigned:
<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	AUSA's Initials: P.E.C.

Case Title: USA v. Aleksandr Grichishkin, et al**County where offense occurred :** Wayne County and elsewhere**Check One:** ☒ **Felony** ☐ **Misdemeanor** ☐ **Petty**☐ Indictment/ ☐ Information --- no prior complaint.☐ Indictment/ ☐ Information --- based upon prior complaint [Case number:]☒ Indictment/ ☐ Information --- based upon LCrR 57.10 (d) [Complete Superseding section below].**Superseding Case Information****Superseding to Case No:** 19-20478**Judge:** Denise Page Hood

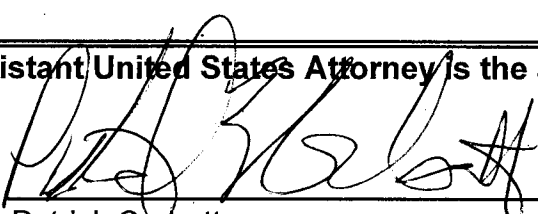
- ☒ Corrects errors; no additional charges or defendants.
- ☐ Involves, for plea purposes, different charges or adds counts.
- ☐ Embraces same subject matter but adds the additional defendants or charges below:

Defendant name**Charges****Prior Complaint (if applicable)**

Please take notice that the below listed Assistant United States Attorney is the attorney of record for the above captioned case.

2/12/2020

Date


 Patrick Corbett
 Assistant United States Attorney
 211 W. Fort Street, Suite 2001
 Detroit, MI 48226-3277
 Phone: 313-226-9703
 Fax: 313-226-4678
 E-Mail address: Patrick.Corbett@usdoj.gov

¹ Companion cases are matters in which it appears that (1) substantially similar evidence will be offered at trial, or (2) the same or related parties are present, and the cases arise out of the same transaction or occurrence. Cases may be companion cases even though one of them may have already been terminated.